Data Security & Privacy Committee Agenda

July 17, 2012 / 10:00 AM – 4 PM

Webinar Registration:
https://www1.gotomeeting.com/register/924229744

Chicago Location:
James R. Thompson Center
100 W Randolph, suite 2-025
Chicago, IL 60601

Springfield Location:
Illinois State Library
Gwendolyn Brooks Building
300 W. Second St., Room 421
Springfield, IL 62701

I. **Roll Call**

II. **Data Security and Privacy Committee Overview**

III. **ILHIE Technical Infrastructure Overview**

IV. **Regional HIE Technical Infrastructure Overviews**

V. **Testimonies – (11:00am-12:00pm)**

Patient Choice: Options and Permitted Uses for Patient Data
Granularity of Patient Data

VI. **Lunch Break (12:00pm-1:00pm)**

VII. **Testimonies (1:00pm-4:00pm)**

Sensitivity of Patient Data: Safeguards for Certain Personal Health Information
Fostering Public Trust in Health Information Exchanges: Enforcement and Mitigation Strategies
Patient Choice and Consent: Operational Protocols
Patient Choice: Current and Future Technologies
Protecting Patient Data: Security Compliance Standards for Health Information Exchanges

VIII. **Adjourn**

July 12, 2012

Re: Patient Electronic Health Data Privacy and Security Policies

The Illinois Health Information Exchange Authority was established by law in 2010, to develop and implement the state-level Illinois Health Information Exchange (ILHIE). The goal of the ILHIE is to enable healthcare providers and professionals to exchange patient electronic health information in a secure environment. By providing authorized electronic access to comprehensive patient medical records, the ILHIE will help to improve patient care, ensure the accuracy of prescriptions and other medical orders, and reduce healthcare costs. Further information regarding the nature and functions of the ILHIE is available at http://hie.illinois.gov.

In connection with the development and implementation of the ILHIE, the Authority is currently developing privacy and security policies relating to the patient data that will be exchanged by the ILHIE. Specifically, the Authority has charged the ILHIE Data Security and Privacy Committee with developing recommendations for possible privacy, security, and consent management policies that may govern the ILHIE. Further information regarding the Committee is available at http://www2.illinois.gov/gov/HIE /Pages/DataSecurityandPrivacy.aspx.

The Committee will hear testimony on the following panel topics on Tuesday, July 17th.

Patient Choice: Options and Permitted Uses for Patient Data

There are different options for patients expressing their preferences regarding the disclosure and use of their electronic health data.

- What patient consent policies should be applied to the operations of the State-level ILHIE?
- Should patients be given a choice whether their electronic patient data is transmitted through an HIE?
- Should they be given a choice with regard to the use and exchange of this data by clinical treatment professionals and others?
- If patients are provided with a choice, should all patients be provided with an option to affirmatively decline (opt-out) or the option to affirmatively consent (opt-in) for exchange of their data through an HIE?

Granularity of Patient Data

Balancing the need for the free flow of health information with a patient's need or desire to determine what information is shared with other parties is one of the main challenges confronting HIEs.

- Should patients be granted the ability to sequester specific elements of their patient record from all providers (or from specific providers)?
- Since most physicians wish to receive and rely only on a complete patient medical record, should the patient's decision not to have certain information shared result in exclusion of the entire patient record from the HIE?

- Should public health authorities have access to a patient's entire medical record?
- Should providers have access to a patient's entire medical record to provide emergency medical treatment?

Sensitivity of Patient Data: Safeguards for Certain Personal Health Information

Patients are generally more protective of their sensitive personal health information, usually because of the potential risks arising from the wrongful use of personal data associated with specific sensitive health issues. Currently in Illinois the following categories of patient health information (PHI) are afforded special patient consent procedures to permit disclosure of such data: HIV/AIDS; behavioral health; substance abuse and genetic testing.

- Should sensitive PHI be treated differently from other types of PHI that are exchanged through an HIE?

Patient Choice and Consent: Operational Protocols

Patients may be concerned about the confidentiality and security of their health information contained in a HIE.

- What is the best way to inform patient choice regarding the risks and benefits of HIEs?
- Should providers have to discuss HIEs with patients such that "meaningful choice" is obtained?
- Or do "Notice of Privacy Practices" accompanied by informative website disclosures suffice?
- Should all consents be written or can consent be obtained orally?
- Once consent is validly obtained, is it valid for an unlimited duration of time?
- Or can it be revoked after a certain amount of time?
- If consent can be revoked how should providers reconcile conflicting patient consents?

Patient Choice: Current and Future Technologies

- Should the state-level ILHIE utilize a unique patient identifier for the purpose of matching patient records?
- To what extent should the state-level ILHIE impose upon providers connected to the state-level ILHIE standards for the degree of patient matching accuracy achieved in provider systems?
- Should patients be able to access their data transmitted through the ILHIE to check for inaccuracies?
- If inaccuracies are apparent, should the ILHIE address patient requests to correct data or refer such requests to the patient's healthcare providers?

Fostering Public Trust in Health Information Exchanges: Enforcement and Mitigation Strategies

If patients do not trust HIEs due to actual or perceived risks they may chose not to have their personal health data available through the HIE.

- Because an HIE's success is directly related to patient participation, what sort of mechanisms should be in place to foster public trust in HIEs?
- What sort of enforcement monitoring is most practical?
    - Breach reporting?

    - Real time network monitoring?
    - Field monitoring?
- Or a combination of all three?
- If a breach does occur, what are the proper strategies for breach mitigation?
- Also, what is the best way to show the public that these mechanisms and strategies are in place to protect patient data?

<u>Protecting Patient Data: Security Compliance Standards for Health Information Exchanges</u>

Protecting patients' privacy and securing their health information is imperative to building patient trust, which is a requirement to realizing the full potential of HIEs.

- To build trust by protecting patient data, what restrictions should there be on permitted uses of data by HIEs?
- Which entity or entities should establish and impose security compliance standards on HIEs?
- Should ILHIE impose such standards on sub-State HIEs?